UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

BMG RIGHTS MANAGEMENT (US) LLC, and ROUND HILL MUSIC LP, Plaintiff, v. COX ENTERPRISES, INC., COX COMMUNICATIONS, INC., and COXCOM, LLC, Defendants.	)	Case No. 1:14-cv-1611 (LOG/JFA)

DECLARATION OF WILLIAM ROSENBLATT IN SUPPORT OF DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

NON-CONFIDENTIAL VERSION

TABLE OF CONTENTS

1. I, William Rosenblatt, submit this declaration pursuant to 28 U.S.C. § 1746.

I. QUALIFICATIONS

2. I am president of GiantSteps Media Technology Strategies, a consultancy that I formed in June 2000. GiantSteps consults on technology strategy related to digital content with particular emphasis on digital rights technologies, digital content management, and the Internet.

3. My involvement in these fields dates back to 1994, when I was Director of Publishing Systems at Times Mirror Co. I represented the company on a publishing industry committee responsible for developing pro-competitive standards to address the emerging issue of online copyright management. I was one of the designers of the standard that came out of this initiative, the Digital Object Identifier (DOI). The DOI is widely used today, primarily in academic and scientific publishing.

4. As a consultant, my clients have included companies from across the spectrum of digital rights and online content issues, including technology companies (ranging from early-stage startups to companies like Microsoft, IBM, and HP), online service providers (including telephone companies, cable television operators, and providers of Internet content services), and copyright owners (including major film studios, record labels, and various types of publishers). I have consulted to several companies specifically on subject matter related to content recognition, content identification, and technical measures used by copyright owners to protect copyrighted works.

5. I have also testified before, or provided consulting to, public entities including the Copyright Office, Federal Trade Commission, National Academies, and European Commission, as well as advocacy groups such as the Business Software Alliance and Association of American Publishers, in all cases on issues related to copyright in the digital age.

6. I am the author of *Digital Rights Management: Business and Technology* (Wiley, 2001), the chapter "Digital Rights and Digital Television" in *Television Goes Digital* (Springer, 2010), and several white papers and articles on digital rights and online content. I was editor of the online newsletter DRM Watch from 2001-2009, and I have published the blog Copyright and Technology since 2009.

7. I have chaired the Digital Rights Strategies and Copyright and Technology conferences from 2004 to the present. I have spoken on related subject matter at conferences on five continents, including the World Economic Forum (Davos); Congressional Internet Caucus State of the Net; National Association of Broadcasters; Book Expo America, International Copyright Technology Conference (South Korea); SET (Sociedade de Engenharia de Televisão, Brazil); European Union Online Content for Creativity (Slovenia); Les Assizes du Livre Numerique (France), Progress and Freedom Foundation Aspen Summit; ACM Computers, Freedom, and Privacy; and various others. One of the presentations I have given, which was produced to Plaintiffs in this case, was on techniques for automating DMCA notice-and-takedown processes, given in 2007 to an audience of Congressional staffers and people from lobbying organizations in Washington. I have guest lectured on digital copyright at several colleges and law schools. I have been quoted on related subject matter in publications in eight countries including The New York Times, The Guardian, Der Spiegel, Billboard, and various trade publications.

8. My experience with Internet technologies dates back to 1985, when I was employed as an engineer at a company (Intermetrics Inc., now L3 Communications) that did software development work for government and defense clients, and thus had access to ARPANET, a direct precursor to the Internet.

9. My educational background includes a B.S.E. in Electrical Engineering and Computer Science, *cum laude*, from Princeton University (1983), an M.S. in Computer and Information Science from the University of Massachusetts (1990), and PhD coursework and research at University of Massachusetts in programming languages, databases, and software engineering.

10. I worked as a software engineer at Motorola and Intermetrics (see ¶ 8 above) between college and graduate school. I have written software in several programming languages for a total of over ten years.

11. I have previously submitted three expert reports in this matter. The Expert Report of William Rosenblatt dated June 19, 2015 is Exhibit C to this declaration ("Rosenblatt Opening"). The Rebuttal Report of William Rosenblatt dated July 10, 2015 is Exhibit D to this declaration ("Rosenblatt Rebuttal"). The Reply Report of William Rosenblatt dated July 24, 2015 is Exhibit E to this declaration ("Rosenblatt Reply").

12. My CV is Exhibit B to this declaration. A tutorial on the relevant aspects of the underlying technologies that are pertinent to this case is provided as Exhibit A to this declaration.

II. OVERVIEW OF ISP INDUSTRY PRACTICES WITH RESPECT TO THE DMCA.

13. I understand that an online service provider may qualify for limitations on copyright liability ("safe harbor") under 17 U.S.C. § 512 if it meets certain definitional and other criteria. There are four safe harbors set forth in §§ 512(a) through (d). Certain of the criteria for these safe harbors – as set forth in the applicable subsection of § 512 – depend on the kind of services that the provider offers.

14. Like most other ISPs, Cox offers various Internet services – including email (see Exhibit A ¶17), online file storage, and others – in addition to its basic ISP functions (see Exhibit

A ¶15). Yet I understand that Cox's basic function as an ISP is at issue in this case. Therefore my analysis focuses exclusively on this function, except where noted below.

15. ISPs in the United States have generally chosen to seek the § 512(a) safe harbor for "[t]ransitory [d]igital [n]etwork [c]ommunications." Toward that end, they have evolved a set of best practices related to adopting policies and processes to satisfy the qualification requirements given in 17 U.S.C.§ 512(i). These are that a service provider --

> "(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
>
> (B) accommodates and does not interfere with standard technical measures." (17 U.S.C. § 512(i)(1).)

16. As I understand it, the § 512(a) safe harbor does not specify steps that ISPs must take to address allegations of copyright infringement on their networks. Yet the § 512(c) safe harbor for "[i]nformation [r]esiding on [s]ystems or [n]etworks [a]t [d]irection of [u]sers" (for what are generally known as "hosting services") does spell out such steps. These include requirements for "respond[ing] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity" (§ 512(c)(1)(C)) as identified in notifications of claimed infringement that include certain information elements described in § 512(c)(3). Such notices are commonly known as "DMCA notices" or "takedown notices."

17. Although ISPs are not hosting services and therefore do not control "access to[] the material that is claimed to be infringing or to be the subject of infringing activity", many ISPs have chosen to adapt the steps specified in § 512(c) for their own use for purposes of the § 512(a)

safe harbor; such steps include accepting notices that conform to the information elements set out in § 512(c)(3) as well as other requirements the ISPs may choose to establish for notices. The notices that these ISPs accept for alleged copyright infringement resemble notices sent to other types of online service providers (such as hosting services) so closely that copyright complainants can use the same standard machine-readable format for notices to ISPs as they do for notices to other types of services (Rosenblatt Rebuttal ¶92).

18. In my experience, all major ISPs in the United States have adopted and publicized the § 512(c)(3) notice requirements for purposes of the § 512(a) safe harbor (Rosenblatt Opening ¶48). In fact, the uniformity with which ISPs accept such notices has engendered a competitive industry of copyright enforcement service providers, which monitor various online services for possible infringements of their clients' copyrighted works and send similar notices to ISPs as well as other types of service providers. Rightscorp, which works with the Plaintiffs in this matter, is one such enforcement service provider. Others include MarkMonitor (see ¶26 below); CEG TEK, a/k/a Copyright Enforcement Group (see ¶91 below); Vobile (see ¶92 below); Entura, Irdeto (a/k/a BayTSP); and IP-Echelon (Rosenblatt Reply ¶81).

19. These enforcement service providers originally earned revenue by charging copyright owners fees to monitor for potential infringements of their works, and many still do. Rightscorp is one of a few more recent entrants into this market that attempt to collect monetary "settlements" from ISP account holders in lieu of lawsuits for copyright infringement. Because ISPs keep the identities of their account holders private (see Exhibit A ¶10), such enforcement service providers ask ISPs to forward "settlement offers" to account holders whose IP addresses they include in notices to the ISPs. In the settlement offers, account holders are offered the chance to pay a fee in order to be released from potential liability for infringement; the copyright

enforcement service provider typically collects the fees and splits them with the owners of the works alleged to have been infringed. The settlement offers typically include web links and phone numbers that account holders can call to discuss the matter.

20. As I understand it, the § 512(i) qualification requirements neither include nor refer to any definitions of "repeat infringer" or "appropriate circumstances"; therefore, ISPs have similarly evolved practices with respect to these terms that imply such definitions.

21. For example, there is understood to be ambiguity about whether the "infringers" in "repeat infringers" are users who have been adjudicated to have infringed copyrights, or who merely have been alleged to have infringed. At least two major ISPs have adopted policies and/or processes based on the former definition: AT&T has stated publicly that it will "terminate 'repeat infringers' in appropriate circumstances" only "in response to … conclusive determinations of infringement by a court",[1] [redacted]

22. Similarly, there is understood to be ambiguity about the meaning of "repeat." For example, Suddenlink states that it "does NOT have a rigid, one-size-fits-all termination rule. Instead, we treat each case individually and work with our customers to resolve allegations of copyright infringement long before we ever consider terminating service."[2]

23. A more comprehensive and established example of ISPs' practices with respect to § 512(i) qualification requirements is a set of processes that many of the country's largest ISPs have adopted, in cooperation with major copyright holders, called the Copyright Alert System ("CAS"). More detailed descriptions of CAS can be found at Rosenblatt Opening ¶¶74–98 and Rosenblatt Rebuttal ¶¶34-47; here is a brief summary.

[1] http://www.businessinsider.com/att-wont-disconnect-over-six-strikes-2013-9.

[2] http://help.suddenlink.com/internet/Pages/DMCA.aspx#3, capitalization in original.

24. The CAS is a system that participating copyright holders use to send notices of alleged infringement on peer-to-peer file-sharing networks, such as BitTorrent (see Exhibit A ¶16), to participating ISPs. The notices contain information elements that are very similar to those required in DMCA takedown notices (see Rosenblatt Opening ¶¶86-91 for a detailed analysis). ISPs act on these notices according to a process set out in great detail in the CAS Memorandum of Understanding ("CAS MoU"), an agreement among the participating organizations.

25. The organizations participating in the CAS are five of the largest ISPs in the U.S.: Comcast, AT&T, Time Warner Cable, Verizon, and Cablevision, respectively the no. 1, 2, 3, 4, and 8 largest by subscribership as of mid-2015. (Charter and Suddenlink, mentioned above, are no. 6 and 10 respectively.)[3] In fact, [redacted] Copyright holders are represented in the CAS by the Motion Picture Association of America (MPAA), Recording Industry Association of America (RIAA), and representatives of independent film, television, and music creators. The CAS is run by an organization called the Center for Copyright Information ("CCI"); the system launched in 2013. (Rosenblatt Opening ¶¶75-76.)

26. MarkMonitor (see ¶18 above) was engaged to run the monitoring and complaint generation processes for CAS. It monitors activity on peer-to-peer file-sharing networks for possible infringements. It uses a combination of technologies and processes (described in Rosenblatt Rebuttal ¶¶36-47) to determine the identity of files being shared. If the identity of a file matches a database of copyrighted works, then MarkMonitor collects data about the possible infringement, including the IP address of the alleged file-sharer, and determines which ISP

[3] http://www.leichtmanresearch.com/press/081815release.html.

assigned that IP address (see Exhibit A ¶10). Then, subject to the rules in the CAS MoU, MarkMonitor sends a complaint to that ISP.

27. The CAS process specifies a series of six actions, called "copyright alerts," that an ISP will take regarding account holders when it receives complaints from MarkMonitor. For the first and second copyright alerts, the ISP sends the account holder warning messages that contain information about the alleged infringement. For the third and fourth, the ISP sends notifications that require the account holder to take an action, such as clicking through warning messages in "pop-up windows" or "landing pages," or watching educational videos on his web browser, before normal Internet service is resumed. These first four alerts are sent no more frequently than once per week, and each alert represents an arbitrary number of complaints regarding the relevant ISP account during the past week.

28. For the fifth and sixth copyright alerts, after a two-week grace period to allow the user to contest the alerts according to a multi-step review process, the ISP takes actions that temporarily interrupt or impair the account holder's Internet access. These precise actions will vary by ISP, but they can include reductions in the account holder's bandwidth for periods of 2-3 days (Verizon), one-day suspension of Internet service (Cablevision), or alerts placed in web browsers that remain there until the account holder calls the ISP's customer service (Comcast) (Rosenblatt Opening ¶¶82, 92-97). In no case is an ISP required to terminate an account holder's Internet access under the CAS (Rosenblatt Opening ¶98).

29. This type of multi-step process, with escalating consequences for account holders, is widely used among ISPs in the United States and elsewhere, both by ISPs that participate in CAS and ISPs that do not; it is commonly known in the industry as a "graduated response" process (Rosenblatt Opening ¶54).

30. The involvement of major ISPs as well as major and independent copyright holders in CAS implies that it implements a broad, cross-industry consensus set of best practices for detecting and acting on incidents of alleged online copyright infringement. Representatives of both copyright owner and ISP interests have expressed this view: the RIAA has described CAS as a "common framework of 'best practices' to effectively alert subscribers, protect copyrighted content and promote access to legal online content", while a Verizon executive stated that it "builds on existing agreements with several copyright owners to forward their notices of alleged infringement to ISP subscribers" and "will set a reasonable standard for both copyright owners and ISPs to follow" (Rosenblatt Reply ¶87).

31. Cox, as the no. 7 United States ISP by subscribership, is a peer of the ISPs that participate in CAS. Cox considered participating in CAS, but it chose not to because, as discussed below, Cox had already implemented its own graduated response system for processing copyright complaints, including software as well as human processes. Cox did not want to go to the effort and expense of adopting another system (Declaration of Randall J. Cadenhead in Support of Defendants' Motion for Summary Judgment (Dkt. 320) ("Cadenhead") ¶18).

32. Yet although Cox chose not to participate in CAS, Cox's graduated response process is more stringent than the CAS process, as discussed in more detail at ¶¶69-71, ¶80, and ¶¶81-83 below. Most importantly, Cox's process calls for termination of accounts, whereas the CAS does not.

33. In fact, Cox has had a reputation in the industry for being tougher on allegedly infringing subscribers than other ISPs. See for example Cadenhead ¶17 ("Cox was the rare (in fact the only, to my knowledge based on communications with others) Internet company with a reputation of terminating customers who failed to take corrective steps in response to repeated

notices of copyright infringement") and https://torrentfreak.com/cox-disconnects-alleged-pirates-from-the-internet-080930/ ("Cox Communications is taking it one step further [than other ISPs], by disconnecting alleged copyright infringers.").

III. COX SATISFIES THE PREFATORY CRITERIA FOR THE § 512(a) SAFE HARBOR.

34. The prefatory criteria that I understand ISPs must satisfy include meeting the definition of "service provider" in § 512(k)(1)(A), and satisfaction of requirements regarding adoption and implementation of a policy that provides for the "termination in appropriate circumstances of subscribers and account holders … who are repeat infringers" in § 512(i)(1)(A), accommodation and non-interference with "standard technical measures" in § 512(i)(1)(B), and the specific eligibility requirements for service providers regarding "[t]ransitory [d]igital [n]etwork [c]ommunications" in § 512(a). I will explain how Cox, as an ISP, meets each of these requirements.

35. First, an ISP must satisfy the definition of "service provider" in § 512(k)(1)(A). This definition is "…an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Cox's ISP services meet this definition because it performs the functions of an ISP described in Exhibit A ¶15; I understand that Plaintiffs do not dispute this, and I describe further in Rosenblatt Opening ¶39 how Cox meets this definition.

36. Second, an ISP must "accommodate[] and [] not interfere with standard technical measures" (§ 512(i)(1)(B)). My understanding is that Plaintiffs do not dispute that Cox meets this criterion, and I describe in Rosenblatt Opening ¶¶120-123 how Cox meets it.

37. Third, § 512(a) sets out specific requirements for safe harbor eligibility for service providers regarding "[t]ransitory [d]igital [n]etwork [c]ommunications." I understand that Plaintiffs do not dispute that Cox, as an ISP, meets these requirements, and I describe in Rosenblatt Opening ¶¶41-42 how it meets them.

38. Finally, the additional requirements stated in § 512(i)(1)(A) are that "[t]he limitations on liability established by this section shall apply to a service provider only if the service provider … has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers" (§ 512(i)(1)). I understand that Plaintiffs do not dispute either that Cox has adopted such a policy or that Cox "informs subscribers and account holders of [its] system or network of" that policy. Thus, in the remainder of this report, I will focus on the remaining requirement, that Cox has reasonably implemented its policy that "provides for the termination in appropriate circumstances of subscribers and account holders … who are repeat infringers." In my opinion, Cox has done so throughout the periods at issue in this lawsuit.

IV. DESCRIPTION OF COX'S DMCA POLICY AND PROCESSES.

39. In this section, I will describe Cox's repeat infringer policy and the graduated response process that implements that policy. As a preliminary matter, it is important to distinguish between Cox's policy regarding repeat copyright infringement and its processes for implementing that policy. I have found that Cox's policy is to terminate in appropriate circumstances account holders who are repeat infringers. In addition, Cox has a set of processes for handling complaints about various types of abuse on the Cox network, one of which is copyright infringement; this set of processes implements the policy. Cox refers to this set of

processes generically using the industry-accepted term "graduated response system" (see ¶29 above). As I will explain, Cox's graduated response system has automated as well as manual components (Declaration of Jason Zabek in Support Of Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment ("Zabek") ¶5). The processes have evolved over time, but the underlying policy has not changed (Declaration of Joseph Sikes in Support of Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment ("Sikes") ¶12).

40. I also note that Plaintiffs do not distinguish policies and processes in this way; they often refer to Cox's "copyright infringement policies" or "copyright policy" in their Memorandum in Support of BMG Rights Management (US) LLC and Round Hill Music LP's Motion for Partial Summary Judgment (Dkt. 324) ("Plaintiffs' SJ Memo") when actually referring to processes. For example, Plaintiffs' SJ Memo includes phrases such as "Cox's Graduated Response Policy" (Plaintiffs' SJ Memo p. 8), "Cox modified its policy" (Plaintiffs' SJ Memo p. 2), and various others. At the same time, Plaintiffs' SJ Memo also refers to Cox's "multi-step, 'graduated response' process for copyright infringement" (Plaintiffs' SJ Memo p. 9), "graduated response procedure" (Plaintiffs' SJ Memo p. 12), and "abuse procedures" (Plaintiffs' SJ Memo p. 14) -- and more ambiguously, "policies and procedures" (Plaintiffs' SJ Memo p. 12).

41. I agree that "procedure" is synonymous with "process" in this case (and indeed Cox uses the terms interchangeably; see generally Zabek). But a process (or procedure) is not the same thing as a policy. An organization can use many different processes to implement a policy regarding something like "termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers," particularly where aspects such as "appropriate circumstances" and "repeat infringers" are not defined.

42. The automated portion of Cox's processes for implementing its abuse policies, including its repeat infringer policy, is implemented in an innovative software system known as the Cox Abuse Tracking System (CATS). [redacted] CATS is described in detail in Declaration of Brent K. Beck in Support of Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment ("Beck"); the following is a brief summary of the aspects of CATS that result in subscriber-facing actions (actions that directly affect Cox's account holders). Although CATS also handles complaints for forms of abuse such as spam, "phishing" (attempts to gather personal information under false pretenses), malware (e.g., viruses), excessive bandwidth usage, and so on, my discussion is limited to CATS's functionality regarding copyright complaints, except where noted below.

43. CATS receives notices of alleged copyright infringement via the email address abuse@cox.net. Cox also accepts copyright complaints via postal mail and fax; Cox employees can also enter complaints into CATS manually if Cox receives them by those means. (Beck ¶3.) As noted above, Cox has adopted the practice of receiving notices in a manner similar to other types of service providers, such as hosting services, that seek to limit copyright liability via the § 512(c) safe harbor (see ¶¶16-17 above). And like those other service providers, Cox acts on complaints of alleged copyright infringement rather than on adjudications by a court of infringement (see ¶21 above).

44. CATS processes copyright complaints to extract certain simple types of information and generates a "ticket," which is an entry in a database that contains the information it has been able to extract through such processing, such as a timestamp and the IP address at

which the infringement was alleged to have taken place. If multiple complaints regarding a given account holder come in within a single day, these are all associated with the same ticket. (Beck ¶¶3-8.)

45. Cox has established certain rules for form and content of abuse complaints. CATS is able to check for compliance with some of these rules automatically, such as the presence of the IP address at which the allegedly infringing activity took place, a timestamp, and an email address of the complainant. It is also able to check for the presence of a valid digital signature, which is a string of data that verifies the identity of the sender of the complaint, designed to meet the requirement of "[a] physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed" (adopted from § 512(c)(3)(A)(i)). (The digital signature is a common requirement in DMCA notices among various types of online services.) (Rosenblatt Rebuttal ¶¶84-86.) Yet even a complaint without a digital signature can be processed manually in Cox's graduated response system; the automated digital signature validation is merely required to enable automated processing (see ¶58 below). (Beck ¶¶6-7.)

46. If the automated compliance tests pass, then CATS may go on to process the complaint in an automated fashion according to the graduated response process (see below); otherwise the ticket will be processed manually. (Rosenblatt Rebuttal ¶¶83-86 and ¶¶98-99.) In fact, based on recent data, CATS takes automated action on about 89% of tickets (Beck ¶4).

47. Compliance with other rules cannot reasonably be tested automatically. One such rule, of importance in this litigation, is that complaints cannot contain content that Cox deems objectionable, including obscenities and "settlement offers" (see ¶19 above). Cox's legal department determined that the latter, in complaints sent by Rightscorp, were "… extra-legal

threats of loss of Internet service and accompanying demands for money [paid to Rightscorp] to avoid such loss [that] relied on improper threats and incomplete and inadequate facts and claims, and therefore were … more like Internet scams, similar to extortion and possibly 'phishing'", and "were not consistent with either the letter or spirit of the DMCA and the safe harbor thereunder as it might apply to Cox." (Cadenhead ¶19.) Thus, complaints with language describing settlement offers are determined to be improper.

48. Because it is possible for notices with such language to make it through the automated testing (and thus be subject to automated processing), Cox has opted to "blacklist" complaints from entities that, even after discussion with Cox, will not remove the improper language. This means that Cox will delete emails sent to abuse@cox.net by those complainants and not enter the complaints into CATS. (Beck ¶17.) I understand that Cox engaged with multiple complainants in this manner, and I have seen over a dozen email addresses whose copyright complaints Cox has blocked due to "settlement offers" and other types of noncompliance with Cox's notice rules. (Rosenblatt Reply ¶28.)

49. Cox's graduated response process (for all abuse types) is largely documented in "Customer Safety and Abuse Operations: Residential Abuse Ticket Handling Procedures," also known within Cox as the "Methods and Procedures" or "M&Ps" ("M&Ps"), multiple versions of which have been produced in this litigation. (The M&Ps apply to Cox residential Internet accounts. A different set of processes apply to Cox's business customers; I understand them not to be at issue and do not consider them here.) The M&Ps document both the subscriber-facing actions that CATS takes and how Cox employees participate in the process by, for example, interacting with account holders on the phone to educate them about complaints, provide assistance in remedying activity at their IP address that has drawn complaints, and determine

when it is appropriate to terminate an account. (Rosenblatt Opening ¶49.) Other aspects of the process are communicated verbally to Cox employees through training and other venues (Zabek ¶13).

50. The graduated response process consists of a series of steps, not unlike the steps in the Copyright Alert System process discussed above. After mapping an IP address to an account holder (see Beck ¶7), [redacted]

51. The following description is a summary of the more detailed description in Zabek ¶9 (see also Rosenblatt Opening ¶¶51-61). It applies to the latest version of the M&Ps, version 4.0, dated October 18, 2012 (Zabek ¶9).

52. [redacted]

[redacted]

53. [redacted]

54. [redacted]

55. [redacted]

[redacted]

56. [redacted]

57. The number of steps and the amount of processing that takes place automatically instead of manually have varied over the years (see Zabek ¶12), as Cox has sought to expand automation where it makes sense to maximize the throughput of the overall graduated response process (Declaration of Jason Zabek in Support of Defendants' Motion for Summary Judgment, Dkt. 321, ¶10).

58. The highest degree of automation in Cox's graduated response process occurs with notices sent by certain complainants that send a large enough volume of complaints to merit automated processing and whose complaints are determined, by Cox's counsel, to be compliant with Cox's rules. Cox has referred to such entities informally as "trusted complainants." Cox routinely communicates with complainants to help ensure that their notices are all proper and to help control the volume of complaints so that Cox is able to process them most efficiently. (Zabek ¶¶26-30 and ¶34; Rosenblatt Rebuttal ¶¶83-88; Rosenblatt Reply ¶¶35-37 and ¶¶66-67.)

59. Yet even with trusted complainants, [redacted]

60. [redacted]

61. [redacted]

62. [redacted]

63. [redacted]

64. [redacted]

65. [redacted]

[4] [redacted]

66. [redacted]

V. COX'S IMPLEMENTATION OF ITS REPEAT INFRINGER POLICY IS REASONABLE.

67. As mentioned at ¶20 above, § 512(i)(1)(A) is non-specific as to the meaning of "termination in appropriate circumstances." To judge the reasonableness of a service provider's implementation of its repeat infringer policy, it is therefore necessary to examine the overall processes that the service provider uses to determine whether account holders are subject to termination "in appropriate circumstances." Having examined Cox's overall processes, I believe that Cox has established and evolved processes that are reasonable in determining appropriate circumstances in which to terminate an account, and thus that Cox ISP account holders are subject to a realistic threat of losing their Internet access as a result of repeated copyright complaints.

68. First, Cox's processes act on notices of alleged copyright infringement (see ¶43 above), rather than only on adjudications of infringement, which means that account holders who are the subject of repeated complaints of infringement are subject to a higher risk of termination than if repeated adjudications in court against the account holder were required. This is in line with standard practice for many major ISPs (see ¶17 above) and is stricter than the practice of those major ISPs that require adjudications (see ¶21 above).

69. Second, Cox's processes are at least as stringent as those of its peers among major American ISPs that participate in the Copyright Alert System. I described the Copyright Alert System at ¶¶23-30 above.

70. As mentioned at ¶32 above, the most important point of differentiation between Cox's graduated response process and the CAS is that Cox's processes both contemplate and lead to actual terminations of ISP accounts, while CAS's do not. Table 1 provides a more complete comparison between Cox's process – the most current version of it (see ¶51 above) – and CAS. It shows that, in addition to terminating account holders in appropriate circumstances, Cox's process is more stringent in that it calls for no grace period before taking an action that affects the user's Internet access, instead of a two-week grace period; and it takes each subscriber-facing action based on one day's worth of complaints instead of a week's worth of complaints.

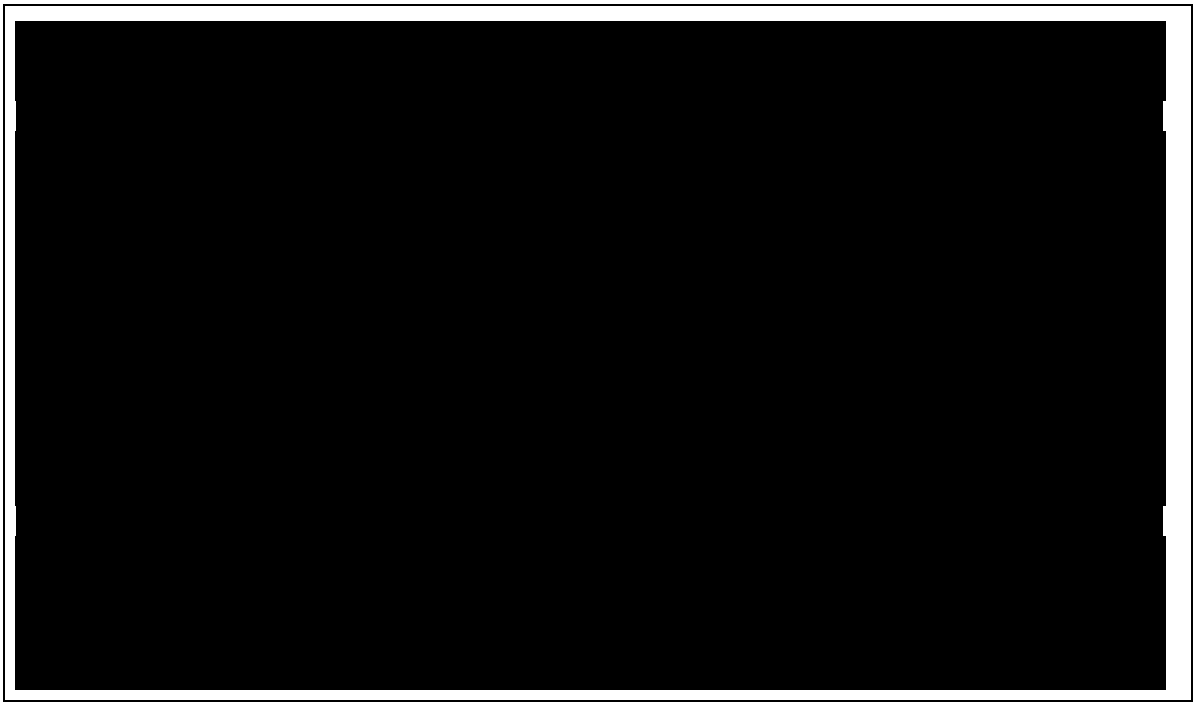


Table 1: Comparison of Copyright Alert System with Cox's Copyright Graduated Response Steps.

[5] In this and subsequent entries for Cox, the first number refers to actions taken on accounts that do not have email addresses on file, and the second number refers to actions taken on accounts with email addresses on file.

[6] ISPs representing 40% of the total subscribership of ISPs participating in CAS. See *supra* note 3.

71. The fact that the major media industries as well as independent copyright holders have agreed to adopt, support, and endorse the CAS (see ¶33 and ¶38 above) indicates that a broad cross-section of copyright owners have accepted the CAS procedures as reasonable practices. Because Cox's scheme is at least as stringent as the CAS procedures, it must also be reasonable according to widely accepted industry conventions.

72. Apart from the comparison with CAS, I believe that Cox's graduated response process is reasonable for a number of other reasons. First, it makes sense to have a number of steps in a process that may ultimately result in the termination of an account due to copyright complaints. Although ISPs are obviously not in a position to adjudicate allegations of copyright infringement, it is reasonable for them to take steps to help the account holder understand possible conditions or activity that may have led to the complaints and to assist the account holder to determine whether he can take his own steps to stop activity that could give rise to future complaints. It follows that it is reasonable for Cox's process to combine automation with human training and interaction with account holders.

73. Through its experience, Cox has found that there are several reasons why an account holder himself may be wrongly accused of infringement. Cox has found that many account holders do not understand why they have received warnings or suspensions, and may need education or assistance in taking steps to eliminate conditions that give rise to copyright complaints (Rosenblatt Opening ¶67, Zabek ¶9 and ¶¶12-18).

74. As a technical matter, copyright complaints target IP addresses, each of which an ISP like Cox can map to accounts (see Beck ¶7); yet many different devices (operated by different people) can access the Internet through an ISP account at any given time (see Appendix A ¶12). One source of copyright complaints that Cox has found to be particularly common is open Wi-Fi

(see Exhibit A ¶¶13-14), which affords opportunities for people unknown to the account holder to use an ISP account for nefarious activities without the account holder's knowledge. Another is that a file-sharing program, such as a BitTorrent client (Rosenblatt Rebuttal ¶¶20-29), is running on a device connected to the Internet through an account holder's cable modem unbeknownst to him. Yet another is a virus or other "malware" on account holders' devices that generates activity that draws complaints. Accordingly, Cox trains its customer service representatives to diagnose such issues and interact with account holders accordingly (Zabek ¶9).

75. In other cases, copyright complaints can target an activity that has no tangible relationship to the account holder's equipment. Evidence produced in this litigation provides examples of this. One is a complaint sent by a [redacted] (Declaration of Andrew P. Bridges in Support of Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment ("Bridges") Ex. 25.) (Rosenblatt Opening ¶68.)

76. Accordingly, Cox takes steps to engage with account holders over accusations of infringement that reasonably escalate in their effectiveness at "getting their attention" and causing them to take action. These steps proceed from advisory messages (warnings) through increasingly intrusive interruptions in service before they come to account termination. As discussed below (¶¶105-111), these steps appear to be effective in sharply reducing the activities that draw copyright complaints.

77. I note that Rightscorp appears to agree that service suspension is a reasonable penalty to impose as part of a copyright complaint process. As mentioned at ¶19 above,

Rightscorp asks ISPs to forward "settlement offers" to account holders whose IP addresses it includes in copyright complaints. Rightscorp also asks ISPs to suspend those account holders' Internet service until the account holders pay the monetary settlements.

78. Furthermore, Cox is consistent about the resources it provides to account holders throughout the process to help them address infringement complaints. These resources include information it provides on web pages to subscribers independently of the copyright complaint process (Cox publishes a guide to wireless security on its website, which anyone can access anytime), information on web pages or in email messages during the process, information and assistance from customer support representatives during the process, and warnings about consequences of failing to correct activity that has led to copyright complaints, i.e., warnings about account termination. (Rosenblatt Opening ¶69, Zabek ¶¶9-12.)

79. I also believe that it is more effective not to communicate the specifics of steps in a graduated response process, as Cox has elected not to do, because that makes account holders less inclined to "game the system" by knowing that there is a certain level of potentially infringing activity that they can get away with before incurring penalties such as suspensions and terminations. I note that Cox's process is superior to the Copyright Alert System in this respect (the CAS process is published at http://www.copyrightinformation.org/the-copyright-alert-system/), and that Cox is not alone among major ISPs in choosing not to communicate such process details; Suddenlink, another major ISP that appears to use a graduated response process outside of the CAS (see ¶42 above), does this as well (see ¶22 above).

80. [redacted]

[redacted] Automation through CATS has enabled greater throughput than what would be possible with manual processing while retaining reasonable safeguards against abuse of the process, overloading of the system (Zabek ¶27), and suspension or termination of accounts in inappropriate circumstances. Moreover, although I understand that Cox has added resources to CATS on a regular basis to keep up with the increase in abuse complaints (Rosenblatt Reply ¶80), I agree that scaling the system in this fashion is a nontrivial matter for the reasons that Mr. Beck suggests (Beck ¶26).

81. [redacted] they give participating ISPs latitude about when resource constraints compel them to cease processing those notices. The following analysis restates Rosenblatt Reply ¶¶90-91.

82. According to the CAS MoU, the major film studios (collectively) and major record labels (collectively) each have limits on the number of notifications that can be sent on their behalf to ISP participants per month. The magnitude of these limits is not specified in the CAS rules, but an independent source has estimated the total limit for Comcast to be "a little under 2,000 notices per day" across all participating copyright owners.[7] [redacted] (Cox's Response to Plaintiffs' Interrogatory No. 5.)

[7] https://torrentfreak.com/comcast-sent-1000000-copyright-alerts-to-pirating-subscribers-141109/.

83. In addition, according to the rules in the CAS MoU, participating ISPs have the option to process fewer notifications than the limits described above if they determine that they are receiving more notices, or calls from account holders regarding those notices, than they "can reasonably address (taking into account the other demands on Participating ISP customer service representatives for unrelated purposes)" (Rosenblatt Reply ¶91 citing CAS MoU p. 16). According to these rules, ISPs have even more leeway under CAS than Cox does under its own stated processes and [redacted] This is yet another respect in which Cox's graduated response system for copyright complaints is more onerous than the CAS.

84. I note that I did not, in my expert reports in this case, [redacted]

85. First of all, it is unreasonable to do the opposite – to let complaints accumulate throughout a person's tenure as an account holder. Were complaints to accumulate indefinitely, the longer one holds an account on an online service, the more likely it is that his account will be subject to termination for alleged abuse (not to mention that penalizing customers for loyal patronage is the diametric opposite of good business sense).

86. Beyond that, the use of [redacted] is not only reasonable but common. One example is "points" assigned to a driver's license for motor vehicle violations: many states allow points on a license to expire after a certain period. The rules vary from state to state, but some examples include 18 months

for New York[8] and 12 months for Pennsylvania,[9] while schemes in other states such as Virginia[10] and New Jersey[11] call for reductions from point totals after one year of violation-free driving.

87. More to the point, the Copyright Alert System rules call for a similar "reset" after 12 months (CAS MoU, p. 13). I do not view the difference between this [redacted] Recall, for example, that the CAS rules limit copyright alerts sent to ISP account holders to one per week and insert a two-week grace period before the fifth and sixth CAS alerts (see ¶28 above). In addition, account holders have the option to dispute a fifth or sixth CAS alert. In that case, a multi-step review process specified in the CAS rules can add as much as 65 days to the process per dispute, for a total of over two and a half months for each alert (CAS MoU pp. 26-35). In contrast, a Cox account holder who engages in persistent allegedly infringing activities may be terminated [redacted] I therefore disagree with Plaintiffs' assertion that "[a]ccumulating so many notices is itself almost impossible because the [redacted] strikes do not include [redacted] (Plaintiffs' SJ Memo p. 27).

88. In all, I disagree with Plaintiffs' characterization of Cox's processes as "designed to limit the circumstances in which Cox will learn of infringement on its system" (Plaintiffs' SJ

[8] http://dmv.ny.gov/tickets/about-nys-driver-point-system.

[9] http://www.dot.state.pa.us/Public/DVSPubsForms/BDL/BDL%20Manuals/Manuals/PA%20Drivers%20Manual%20By%20Chapter/English/chapter_4.pdf.

[10] http://www.dmv.state.va.us/drivers/#points_you.asp.

[11] http://www.state.nj.us/mvc/Violations/penalties.htm.

Memo p. 22) or "designed and implemented to avoid terminating repeat infringers at all" (Plaintiffs' SJ Memo p. 25).

89. Now I turn to the rules, mentioned at ¶45 above, that Cox has established for form and content of abuse complaints that must be complied with for Cox to process them (manually or automatically). Cox is reasonable in setting such requirements. To begin with, it is reasonable for Cox to use automated means to reject messages sent to abuse@cox.net that are clearly not intended as copyright complaints (e.g., spam). Beyond that, as the operator of a system that must handle a very large volume of abuse complaints, it is reasonable for Cox to set rules that complainants must abide by before their copyright complaints will be processed. And given that large volume, it is reasonable for Cox to use automation to test for compliance with those rules that can pragmatically be tested that way (see ¶45 above) and for the rules to include those that are not easily tested automatically. And it is reasonable for the rules to preclude notices that contain language that is offensive to Cox's subscribers or that Cox judges to be scams, extortion, or phishing.

90. At the same time, it is also reasonable for Cox to attempt (as it did) to work with copyright complainants to eliminate objectionable language from their complaints rather than to attempt to modify complaints itself to eliminate objectionable language from them. Cox has worked with complainants in this manner, often to mutually satisfactory outcome. The following examples (and counterexample) restate Rosenblatt Reply ¶¶66-68.

91. The first example is CEG TEK, a company in a similar business to that of Rightscorp (see ¶19 above). CEG TEK was initially sending complaints to Cox that contained settlement offers. At first, Cox blocked the complaints. Then CEG TEK responded by sending copyright complaints without settlement offers, which Cox processed automatically. Yet at a later

point, CEG TEK attempted to "sneak in" settlement offers to their modified complaints. Like some other copyright complainants, CEG TEK uses a machine-readable standard format for copyright complaints from the MPAA called Automated Copyright Notice System ("ACNS"). CEG TEK had adopted the tactic of "sneaking" URLs that linked to web pages containing settlement offers into its ACNS-formatted complaints, so that Cox account holders who received warning emails (see ¶50 above) would see these URLs and possibly click on them to view the settlement offers. Cox discovered this and subsequently blocked CEG TEK's complaints again. This episode demonstrates that Cox's concerns about abuse of the complaint process are not just hypothetical. I understand that CEG TEK now complies with Cox's standards, and Cox now processes CEG TEK's complaints in an automated fashion as a trusted complainant (Cadenhead ¶20).

92. The other example, which involves more technical considerations, is that of [redacted] And this process of working with complainants is not limited to copyright; Cox uses it for other types of complainants, such as spam detection services.

93. The counterexample is Rightscorp. As I understand it, Rightscorp did not respond to Cox's efforts to work with Rightscorp in this manner; see Cadenhead ¶23 and Zabek ¶32. Rightscorp's notices contained "statements that Cox might terminate Internet service to the account holder if a payment was not made to Rightscorp" (Cadenhead ¶22). Therefore, Cox decided to blacklist (see ¶47 above) complaints from Rightscorp. (Cadenhead ¶¶22-25, Zabek ¶33.)

94. In fact, Rightscorp appears to insist on the inclusion of settlement offers in its copyright complaints [redacted]

95. Moreover, even among the small number of copyright enforcement services that pursue monetary "settlements" from ISP subscribers (see ¶19 above), Rightscorp's practices are unique, in my experience, for including explicit threats to subscribers of interruption of their Internet service – i.e., implications that the ISP (rather than the copyright holder or Rightscorp itself) will take an action against the subscriber if the subscriber does not pay Rightscorp. For example, RGHTS10536724 (Bridges Ex. 1) is a sample Rightscorp notice; like many others produced in this litigation, it contains a statement that "[y]our ISP service could be suspended if this matter is not resolved." (Bridges Ex. 1.) Contrast this with a sample notice sent by CEG TEK ("Copyright Enforcement Group"), which can be seen at http://www.expertlaw.com/forums/showthread.php?t=137751; it mentions potential legal remedies the copyright holder (Metro Media Entertainment) may pursue but does not mention any action that the ISP (Suddenlink, which forwarded the notice to the subscriber) may take regarding the subscriber's account. This is another reason why it was reasonable for Cox to have blacklisted Rightscorp's notices.

96. The example of CEG TEK above illustrates why the burden of modifying complaint notices to comply with a service provider's requirements falls properly on the

complainant. It is too difficult for a service provider to reasonably analyze and "guess" at the objectionable parts of a complaint, especially given the large number of rights holders and enforcement service providers that send notices of alleged infringement to Cox.

97. Cox does process copyright complaints to extract certain simple types of information, to help test for compliance and to store the information in its complaint database. The information extracted typically includes the complainant's email address, the subject line of the email message, the accused IP address, timestamp, and other information expressed in simple character or numerical strings. It also performs simple tests for "good faith" and "penalty of perjury" statements (corresponding to information elements recited in § 512(c)(3)(v) and (vi) respectively). It will also check for the presence of a valid digital signature (see ¶45 above) (Beck ¶6.) I have examined the source code that CATS uses to perform such processing; it is not complex, and the task of developing code to extract this type of information in order to improve the automation of complaints from a trusted complainant is reasonable. Moreover, even if the automatic processing by this code fails, the complaint is presented for manual review, which may conclude that the complaint is compliant and continue with processing. (Rosenblatt Rebuttal ¶98-99, citing CATS source code.)

98. In contrast, it would be much more difficult, complex, ambiguous, and potentially impossible to determine programmatically, for all parties whose complaints are processed through CATS, which parts of a complaint are not compliant with Cox's rules, and delete or modify them before processing them further. This should be especially apparent from the example of CEG TEK, which attempted to "sneak" settlement offers into its copyright complaints after representing that its complaints no longer included them. Objectionable language such as

obscenity and settlement offers is not generally possible for complaint processing code such as that used in CATS to detect reliably (see Beck ¶6 and ¶25).

99. It is much more reasonable for the complainant, which knows its own notice formats better than anyone else, to make the changes. More generally, Cox's practices are based on a position that complaints it forwards to account holders (see ¶52 above) come from a third party, not from Cox itself. If Cox were to modify a complaint in any nontrivial way, that assumption would no longer be valid and Cox would unduly risk misrepresenting the complainant's statements and intentions. (Rosenblatt Rebuttal ¶¶104-106.)

100. In sum, I disagree with Plaintiffs' assertion that "Cox has created a notification system designed to limit the circumstances in which Cox will learn of infringement on its system." (Plaintiffs' SJ Memo p. 22.) On the contrary, Cox's behavior has established that when complainants work with Cox to send compliant notices, Cox processes them diligently according to its graduated response procedures, which I find to be reasonable.

VI. PLAINTIFFS' ARGUMENTS THAT COX'S PROCESSES ARE UNREASONABLE ARE UNFOUNDED AND BASED ON INCORRECT FACTUAL ALLEGATIONS.

101. In this section I address certain arguments made by Plaintiffs that Cox's processes for implementing its repeat infringer policy are unreasonable. First, Plaintiffs argue that Cox had one "copyright infringement policy in place between first quarter 2010 and October 2012" (Plaintiffs' SJ Memo p. 10 ¶37) and then a "revised [] copyright policy" starting "[i]n late 2012" (Plaintiffs' SJ Memo p. 12 ¶50).

102. I disagree with this assertion. As mentioned above at ¶39, Cox's policy throughout both of those periods (as well as before then) has been the same: to terminate in appropriate circumstances account holders who are repeat infringers. It is true that Cox's processes for implementing that policy have changed over the years, including the addition of

steps resulting in the current scheme (see ¶57 above and Zabek ¶12), but the policy has remained the same. Plaintiffs also overstate the importance or impact of process changes through mischaracterization of internal Cox communications. For example, Plaintiffs claim that "Cox revised its copyright policy so that 'now when we terminate Customers, we REALLY terminate the Customer (for 6 months).'" (Plaintiffs' SJ Memo p. 12 ¶50, citing an email message from Mr. Sikes in late 2012.) This statement did not refer to any changes in the process (or "policy"); instead it referred to internal changes in the mechanics of the termination process rather than any changes in actions that the account holder would notice (Sikes ¶¶11-12).

103. It is thus incorrect to suggest, as Plaintiffs have done, that "[i]n late 2012 … Cox revised its policies and procedures to avoid terminations by eliminating any requirement of termination of repeat infringers" (Plaintiffs' SJ Memo p. 12 ¶¶50-51). In fact, Cox did terminate subscribers throughout the period from late 2012 to the present, including the period from late 2012 to the time when the complaint in this litigation was filed (Response to Plaintiffs' Interrogatory Nos. 5-8).

104. Changes in Cox's processes are described in Zabek ¶12 and Sikes ¶¶7-11, and documented in previous versions of the M&Ps (see Rosenblatt Reply ¶¶39-43). The rationale for the changes in the graduated response process, including the number of steps, was to improve education of subscribers and assistance in remedying issues that result in copyright complaints, and was based on the idea that further opportunities for Cox personnel to interact with account holders would result in reductions in behaviors that lead to copyright complaints (Zabek ¶12, Sikes ¶¶7-10).

105. In fact, actual data from CATS implies that the changes that Cox has made in its processes over these periods of time are more, not less, effective in curbing allegedly infringing

behavior. It is not necessary to focus narrowly on the number of accounts that have been terminated per month to evaluate a process's effectiveness at curbing behaviors that lead to allegations of infringement. Nor is Plaintiffs' assertion that Cox "respond[ed] to [redacted] (Plaintiffs' SJ Memo p. 28) necessarily determinative of the effectiveness of Cox's processes. For example, Plaintiffs have identified internal communications suggesting that Cox decided to allow certain accounts to remain after they had reached the last step in the graduated response process, such as those in Declaration of Jeffrey M. Theodore in Support of Plaintiffs' Motion for Partial Summary Judgment (Dkt. 317) ("Theodore") Exs. 18-19, 21, 45. I understand that such cases are rare and exceptional (Zabek ¶9.f.), and in at least some of them, the account holder stopped engaging in allegedly infringing behaviors and/or terminated his account of his own accord (Sikes ¶13). This reinforces the notion that interacting with subscribers and taking actions such as suspending their accounts helps curb allegedly infringing behavior.

106. Because suspensions are more concrete actions for which Defendants have produced data, and because I understand that Plaintiffs are not disputing the data on suspensions, the analysis here (which restates Rosenblatt Reply ¶¶51-56) focuses on them. Cox produced monthly data about CATS subscriber-facing actions as a result of copyright complaints in its responses to Plaintiff's Interrogatory Nos. 5-8. The data begins in January 2010, just before the introduction of the process documented in M&Ps version 3.0, [redacted]

107. Figure 1 below shows [redacted]

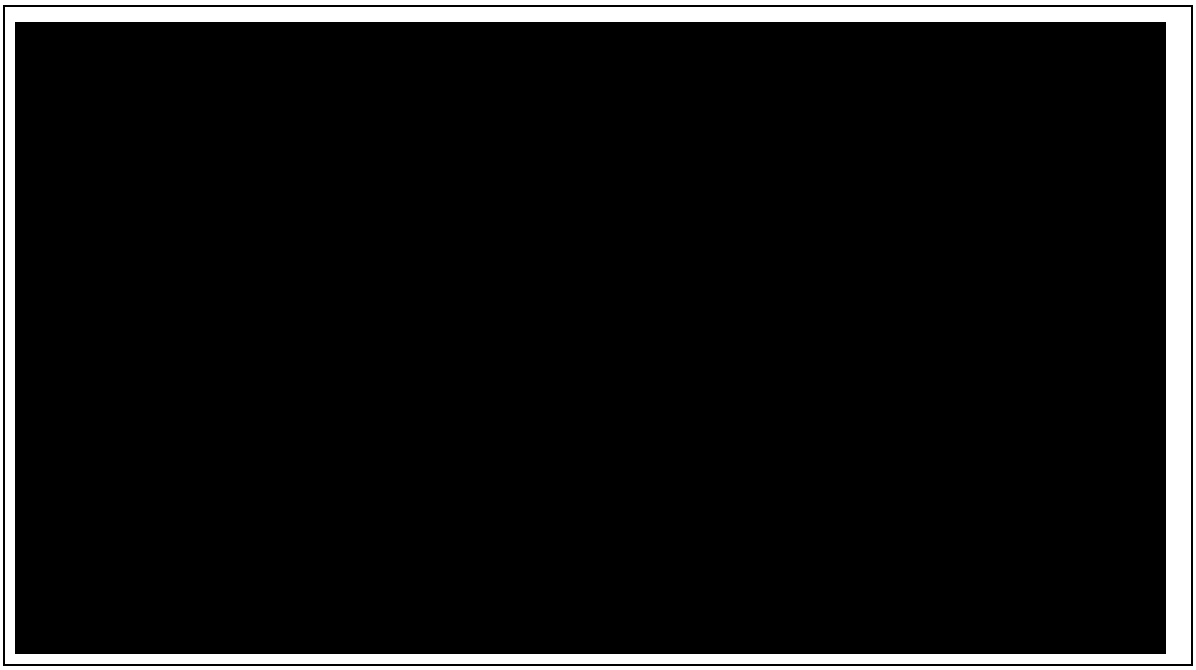


Figure 1:

108. As Figure 1 shows,

109.

[redacted]

110. [redacted]

[redacted]

111. [redacted]

[redacted]

[redacted]

112. Another set of assertions that Plaintiffs have made to support their position that Cox's graduated response process is unreasonable includes statements that "[redacted] Together, these categories account for more than 95% of infringement notices sent to Cox" (Plaintiffs' SJ Memo p. 8 ¶31, citations omitted) and "Cox has taken no action on more than 95% of the copyright notices that it has been sent by copyright owners" (Plaintiffs' SJ Memo p. 24). These statements are both factually incorrect and misleading.

113. First, [redacted] it is incorrect that Cox "take[s] no action" on such tickets. Cox still retains them in CATS in the event that it receives further complaints regarding that subscriber, which could lead to suspensions and termination (see ¶¶52-55 above) (Zabek ¶9).

114. Second, because Cox is reasonable in blacklisting complainants that refuse, after discussions with them, to send notices that comply with its rules (see ¶¶89-95 above), it is misleading to count notices sent by such entities when assessing whether Cox's entire process for

handling complaints is reasonable. There is no basis to suggest that, if those complainants had made reasonable changes to their notices to conform to Cox's rules, that Cox would not have processed and taken action on them as it does for all other compliant notices. In fact, the example of CEG TEK (see ¶91 above) shows just this.

115. Third, Plaintiffs' alleged 95% figure also includes complaints that [redacted]

116. In all, it is more accurate to state that apart from complaints from blacklisted senders, Cox takes some sort of action on all of the copyright complaints it receives by email (Beck ¶9).

117. Plaintiffs cite my deposition testimony that "if Cox's policy were to delete, without any further action or any processing or consideration, every copyright complaint that it received and do nothing else, I would not consider that reasonable." (Plaintiffs' SJ Memo p. 24, citing Deposition of William Rosenblatt, August 18, 2015 (Dkt. 317-9) ("Rosenblatt Depo.") at 14:2-8.) To the extent that Plaintiffs are suggesting that their alleged 95% figure resembles "delet[ing] … every copyright complaint that [Cox] receive[s] and do[ing] nothing else," I disagree. As I have shown, Cox does nothing of the sort, and I stand by my testimony.

118. Finally, Plaintiffs cite a few internal communications among Cox employees as evidence of "an 'under the table' policy of purporting to terminate repeat infringers while actually retaining them" (Plaintiffs' SJ Memo p.1), [redacted] (Plaintiffs' SJ Memo p. 10 ¶38), and "failure to terminate known, repeat infringers in order to preserve the revenue streams associated with their accounts" (Plaintiffs' SJ Memo p. 30).

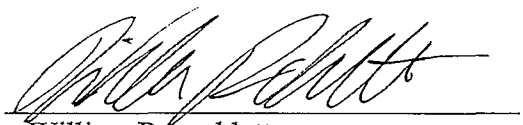
I find Plaintiffs' evidence unpersuasive, indicative more of isolated incidents, practices used rarely and not communicated to account holders, and/or remarks taken out of context rather than of any policy, documented process, or understanding that Cox employees glean through training and other interpersonal communication (Zabek ¶13 and ¶¶23-25). As Mr. Sikes discusses in his declaration, this allegation of "official" and "unofficial" processes is untrue (Sikes ¶12). I described an internal process change that does not affect account holders' perceptions of actions Cox takes against them (despite Plaintiffs' insinuation that it does) at ¶102 above; this includes communications that Plaintiffs have misinterpreted as discussing "reactivation" of terminated subscribers as if it were a Cox policy or standard process; these communications refer instead to internal mechanisms that make it easier to reactivate terminated subscribers on the rare occasion that a decision is made to do so (Sikes ¶11). Another example is the "soft terminati[on]" that Plaintiffs cite at Plaintiffs' SJ Memo p. 11 ¶45. Mr. Sikes describes the rationale for this as an internal convenience rather than anything of which Cox makes the account holder aware (Sikes ¶11). The larger point is that complex processes implemented in the real world, such as Cox's abuse processes, are legitimately subject to occasional variations.

119. I am also unpersuaded by evidence of a few inflammatory comments that certain Cox personnel made regarding their duties under the DMCA; I do not find these indicative of any policy or process, let alone the "'F the dmca!!!' approach to copyright infringement" that Plaintiffs claim exists (Plaintiffs' SJ Memo p. 2). Instead I find it reasonable that people like Mr. Zabek would express frustration, particularly at the fact that DMCA-related copyright complaints in recent years have increased dramatically to become the most frequent type of complaint, imposing demands on constrained resources that are disproportionate to the demands from other types of abuse complaints (Beck ¶26, Rosenblatt Reply ¶80).

120. I also find it reasonable that Cox maintains a balancing act between subscriber retention and its legal obligations regarding copyright infringement (Zabek ¶¶14-18), and that maintaining such a balance may require changes in processes over time. This includes rare decisions, after appropriate deliberation and human discretion, to reactivate subscribers after their accounts have been terminated, and only [redacted] (Zabek ¶¶20-22).

121. To support their allegations that Cox's processes are not reasonable, Plaintiffs have also cited my deposition testimony in order to suggest that I stated that "'it's not appropriate' to 'simply reactivate[] the account that was terminated for an alleged copyright infringement'" (Plaintiffs' SJ Memo p. 26, citing Rosenblatt Depo. at 31:10-32:10 and 37:13-22). This is a misrepresentation of my testimony. The phrase "it's not appropriate" (Rosenblatt Depo. at 32:7) did not refer to "simply reactivat[ing] the account that was terminated for an alleged copyright infringement" (Rosenblatt Depo. at 31:14-16); in fact the latter language was the deposing attorney's, not my own. Instead, "it's not appropriate" referred to my own intervening statement, which was: "Well, I would say that the training that I understand Cox personnel to have -- the relevant Cox personnel to have been given includes training on considering the context. So if they did not consider the context, then that would not be following their training. And so to that extent, I would say, yes, it's not appropriate." (Rosenblatt Depo. at 31:20-32:7.) My actual testimony was thus consistent with the opinions I express herein, and I stand by it.

I declare under the penalty of perjury that the foregoing is true and correct. Executed October 13, 2015.



William Rosenblatt

EXHIBIT A: TECHNICAL TUTORIAL

1. The following tutorial on the relevant aspects of the underlying technologies that are pertinent to this case is largely a restatement of Rosenblatt Opening ¶¶21-36.

2. Consumers and many businesses access the Internet through ISPs (Internet service providers). ISPs can be analogized to telephone companies; in fact many telephone companies (such as Verizon and AT&T) also act as ISPs, in addition to their telephone businesses and using their telephone network infrastructures. Cox is an ISP, though one that offers its services via cable television infrastructure instead of telephone network infrastructure. Other major ISPs that use cable TV infrastructure include Comcast, Time Warner Cable, Charter, Suddenlink, Bright House Networks, and Cablevision. Individuals and entities subscribe to ISP services, including Cox's, by signing up for accounts and, typically, paying monthly fees.

3. Access to the Internet through an ISP requires a piece of equipment called a modem (for "modulator/demodulator"), which sits between a user's device – a computer, tablet, smartphone, etc. – and the ISP. A modem is analogous to the box on the outside of a house that connects all of the telephones in the house to the phone network. ISPs typically supply modems to account holders as part of the process of setting up accounts. Modems used with cable television-based ISPs like Cox are called cable modems.

4. Each modem has an address, a set of numbers called a MAC (Media Access Control) address. A MAC address is analogous to the serial number of a telephone, except that all MAC addresses are unique globally instead of being unique only to the manufacturer of the device. MAC addresses are normally permanent.

5. Devices with Internet connectivity, such as computers, also have MAC addresses. When they connect to the Internet through an ISP, the ISP assigns another type of address to them, a different set of numbers called an IP (Internet Protocol) address. IP addresses are also unique globally, but only with respect to a given point in time, because they are routinely reused or reassigned, as explained below. In other words, the combination of an IP address and a timestamp (a precise indicator of date and time) is globally unique.

6. MAC and IP addresses are both necessary because they serve different purposes. MAC addresses are used at a lower level of communication than IP addresses. The MAC address of one device is normally known only by the next devices in a chain of communication, whereas an IP address assigned to a device may be known to all devices throughout the Internet that communicate with it, including devices internal to ISPs' infrastructures. In addition, MAC addresses are designed to be permanent, while IP addresses are routinely reused.

7. To ensure that no two ISPs assign the same IP address to a device, an organization called the ARIN (American Registry for Internet Numbers) allocates a range of IP addresses to each ISP in North America. The ISP chooses IP addresses from among its given range to assign to users' devices. It keeps track of which IP addresses have been assigned and which are available at any given time. The IP address ranges that ARIN allocates to ISPs are public information; anyone can find out the ISP that assigned a given IP address by querying ARIN's public database.[12]

[12] For example, anyone can go to http://whois.arin.net/ui, enter an IP address, and find the ISP that assigned it.

8. ISPs typically use a scheme called DHCP (Dynamic Host Control Protocol) to assign IP addresses to devices connected to the Internet through their networks. DHCP enables ISPs to assign, or "lease," IP addresses to devices for short periods of time, such as 24 hours, and potentially reuse them when the lease has expired. ISPs maintain logs that record IP addresses assigned to devices (by their MAC addresses), the timestamps of the assignments, and the durations of the leases.

9. To extend the telephone analogy: IP addresses are like phone numbers. Phone companies have sets of phone numbers that they can assign to subscribers. They can reassign phone numbers – to different devices (if the subscriber moves) or to different people (if the subscriber cancels his account). Analogously, ISPs have sets of IP addresses to assign to Internet-connected devices that they can reassign when the assignments or leases expire (and are not renewed). Phone numbers are published in public directories; IP addresses are often discoverable through various Internet-based communications protocols (see, for example, Exhibit A ¶¶15-16). Phones have serial numbers; MAC addresses are like device serial numbers except that they are globally unique instead of unique only to the phone manufacturer; and like telephone serial numbers, MAC addresses are not intended to be known publicly.

10. One important gap exists in the analogy between Internet and phone services with regard to privacy of account information. While it is often possible to obtain the name of a person given a phone number by searching phone directories (a "white pages reverse lookup"), ISPs keep the names and contact information of their account holders private. Accordingly, if someone wishes to contact an ISP regarding a particular user, he must obtain the IP address of the user's device, find the ISP that assigned the address

(through the ARIN database), and send that IP address to the ISP along with the exact time at which he obtained the address. The ISP may be able to search its log of IP address assignments (see ¶7 above) in order to identify the modem through which that IP address was assigned at the time given.

11. Just as it is possible for a telephone account holder to have several phones in his home, all of which use the same phone number and connect through the same phone line, it is possible for an Internet account to have several devices operate through it, all of which would connect to the Internet through the same ISP account and the same modem. A very common way of connecting multiple devices (such as multiple computers, mobile telephones, printers, and the like) to an Internet modem in a home is wirelessly through Wi-Fi;[13] it is also possible to connect multiple devices to a modem with cables.

12. A device that connects multiple devices to a modem is called a router. Most routers used by consumers today accommodate both wireless (Wi-Fi) and "hardwire" (cable) connections. Some modems have router functionality built in. A router manages the data traffic that flows between users' devices and the modem (and thence to and from the Internet in general).

13. An important difference between Wi-Fi and cable connections of devices to routers – apart from Wi-Fi's convenience and portability – is that a Wi-Fi network can be used by any device (with a Wi-Fi network adapter) that is located within the signal range of the Wi-Fi router. Signal ranges of Wi-Fi routers vary widely, depending on

[13] For example, a 2014 study by Strategy Analytics predicted that by the end of 2014, 65% of households worldwide would use Wi-Fi home networks along with residential high-speed Internet connections. https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-broadband-and-wlan-(wi-fi)-networked-households-forecast-2009-2018.

several factors such as the version of the Wi-Fi technology being used, the device's hardware, physical obstructions between the device and the router, other wireless devices (e.g., portable telephones) in the vicinity, etc., but ranges can extend to hundreds of feet and are not necessarily limited by home boundaries. It is easy for unauthorized persons to access Wi-Fi networks, such as from an adjacent apartment, the street in front of a house, from the sidewalk in front of a café, and from a nearby office in an office building.

14. This gives rise to security concerns on Wi-Fi networks. Communications over Wi-Fi networks can be protected by setting passwords or security codes on routers and requiring users to enter the passwords on their devices to connect to the Internet. However, not only is it possible to operate a Wi-Fi network without a password, many people do so; these are often called "open" Wi-Fi networks. One study in 2011 found that 32 percent of respondents admitted that they used other people's open Wi-Fi networks, up from 18 percent in 2008.[14] It is commonly understood in the industry that password setting on Wi-Fi routers is optional; ISPs cannot, as a technological matter, force account holders to set passwords. ISPs generally have no way of determining how Wi-Fi routers are configured, including whether or not they have security features enabled.

15. The basic function of an ISP is to accept traffic consisting of requests, commands, and information from users' devices and route that traffic automatically to the appropriate recipients over the Internet. The requests and commands are given using various types of machine-readable languages called communications protocols, or simply protocols for short. Standard protocols exist for such tasks as email sending and receiving (SMTP and POP3), web page retrieval (HTTP), file transfer (FTP), and so on. There are

[14] The study was conducted by Wakefield Research and the Wi-Fi Alliance. http://www.cnet.com/news/more-people-grabbing-wi-fi-from-their-neighbors/.

also many non-standard[15] protocols used on the Internet for services such as streaming music (e.g., Pandora), streaming video (e.g., YouTube or Netflix), Internet telephony (e.g., Skype), and so on. The identities of recipients are expressed according to the protocol in question, such as email addresses (e.g., billr@giantstepsmts.com), web addresses (URLs, e.g., https://www.law.cornell.edu/uscode/text/17/512), etc. An ISP may store information produced in response to such requests temporarily on its equipment, but only for the purpose of making transmission of the information and the use of the network infrastructure as efficient as possible; any such temporary copies of information are not meant to be accessible to users.

16. One non-standard protocol, BitTorrent, is a protocol for sharing files among multiple Internet users at the same time.[16] For these purposes, the relevant aspect of BitTorrent is that computers that participate in BitTorrent file-sharing make their IP addresses known to one another; this means that if one computer communicates with others using BitTorrent, its software will know the IP addresses of other devices with which it communicates. For more details on BitTorrent, please see Rosenblatt Rebuttal ¶¶20-30.

17. Finally, ISPs typically offer email accounts to their subscribers as an additional service. They do this because of the extreme popularity of email, in order to offer competitive and "complete" feature sets to subscribers. This means that ISPs maintain computers (email servers) that enable users to send and receive email (using the above-named protocols), and they give users email addresses ending in the name of the ISP, such as "cox.net" for Cox or "verizon.net" for Verizon. ISPs' email servers store

[15] By "non-standard" I mean not a standard endorsed by the Internet Engineering Task Force (IETF) or World Wide Web Consortium (W3C).

[16] http://www.bittorrent.org/beps/bep_0003.html.

email messages for subscribers, but these are logically separate from the equipment and processes that enable basic Internet service as described in Exhibit A ¶15. Nevertheless, many account holders do not use their ISPs' email services; instead they use popular ISP-independent email services such as Gmail (from Google) or Hotmail (from Microsoft), or their employers' email services. Analogously, phone companies offer voice mail to customers, but customers may opt to use their own answering machines instead.

CERTIFICATE OF SERVICE

I hereby certify that on October 13, 2015, the foregoing was filed and served electronically by the Court's CM/ECF system upon all registered users.

/s/ Craig C. Reilly

Craig C. Reilly (VSB No. 20942)
111 Oronoco Street
Alexandria, VA 22314
Tel: 703-549-5354
Fax: (703) 549-5355
Email: craig.reilly.@ccreillylaw.com

Counsel for Defendants